

“HTTP状态401 -验证失败：验证SAML消息的错误”，当您使用SSO

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[问题](#)

[解决方案](#)

简介

本文描述您收到一“HTTP状态401”错误消息在休止时期之后的问题，当您使用单一登录时(SSO)。

先决条件

要求

Cisco 建议您了解以下主题：

- SSO
- 活动目录联邦服务(AD FS)
- CloudCenter

使用的组件

本文档不限于特定的软件或硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

当您使用SSO时，如镜像所显示，您能在休止时期之后收到“401”错误，而不是提示符再登陆。

HTTP Status 401 - Authentication Failed: Error validating SAML message

type Status report

message Authentication Failed: Error validating SAML message

description This request requires HTTP authentication.

Apache Tomcat/8.0.29

您的唯一方法能再登陆是关闭整个Web浏览器和重新打开它。

解决方案

这是由不匹配造成的按在CloudCenter和SSO服务器范围的超时值。

增强允许ForceAuthn参数支持，能允许两值和CloudCenter之间的一不匹配温文地注销。此增强可以是被跟踪的此处<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752>。

唯一的应急方案是删除不匹配。有超时值需要配比的三个位置。前两个在CCM。

1. 导航对/usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml。
2. 修改<session-timeout>time_In_Minutes</session-timeout>反射以分钟希望的超时。
3. 导航对/usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties。
4. 修改saml.maxAuthenticationAge.seconds=timeout_in_seconds反射以秒钟希望的超时。

第三在SSO服务器，并且依靠的位置能变化什么类型的SSO服务器运行。Web SSO寿命值必须匹配在CloudCenter配置的两个值。

一旦全部三匹配，当超时出现，您丢弃回到在允许前的登录画面查看页。